IPv6 Mobility in Cluster Based Heterogeneous Wireless Mesh Networks

Huu-Nghia Nguyen, Christian Bonnet
Mobile Communications Department
Eurecom Institute
2229 Route des Crêtes, Sophia Antipolis, France
Huu-Nghia.Nguyen@eurecom.fr, Christian.Bonnet@eurecom.fr

Abstract— **We present a framework for IPv6 mobility support in Cluster Based Heterogeneous Wireless Mesh Networks. The framework inherits the design and the features from the trendy Proxy Mobile IPv6 (PMIPv6) which can provide network-based mobility to Mobile Nodes having standard IPv6 stack. Design and implementation details are described. We also present a virtualization method using User-mode Linux and Ns2-Emultion for implementing and testing the framework. Some qualitative results are provided to prove the correctness and the advantages of our framework.**

Keywords- Proxy Mobile IPv6, PMIPv6, Wireless Mesh Network, Heterogeneous Access, Seamless Mobility .

I. INTRODUCTION

Wireless Mesh Networks (WMNs) are multi-hop wireless networks with self-healing and self-configuring capabilities. These features, plus the ability to provide wireless broadband connectivity, make WMNs a promising solution for ubiquitous Internet access and a wide range of applications [1]. A WMN generally consists of a set of mesh nodes that interconnect with each other via wireless medium to form a wireless backbone. Some or all of the mesh nodes also serve as access points for mobile users under their coverage. One or more mesh nodes have wired connections to the Internet and function as the gateway. Compared to traditional wireless LANs, the main feature of wireless mesh networks is their multi-hop wireless backbone.

We consider a Cluster Based Heterogeneous Wireless Mesh Architecture in which the WMN is divided into clusters as in Fig. 1 that could minimize the updating overhead during topology change due to mobility of mesh nodes. Each cluster containing a Cluster Head (CH) that has complete knowledge about group membership and link state information in the cluster. The cluster head is often elected in the cluster formation process. Other nodes within a cluster, called Access Routers (ARs) in this paper, are minimal mobile and control heterogeneous radio access technologies. A relay router connects two adjacent clusters. A Mobile Node (MN), which attaches to the AR, can be connected through the mesh structure to all other routers in the mesh. The Mobile Node therefore can communicate either with other mobile Correspondent Nodes (CNs) in the WMN through ARs, or with CNs in the Internet through CHs.

We extend Proxy Mobile IPv6 (PMIPv6) to support the seamless mobility in such a Cluster Based Wireless Mesh Network. This approach is advantageous over other existing routing protocols supporting mobility. The architecture can reduce the flooding signaling traffic during the registration process and the dynamic route discovery process, and can support mobility to MNs having unmodified IPv6 stack.

We introduce an IP-Layer attachment and movement detection mechanism to support a heterogeneous environment composed of different access technologies. Upon any attachment of an MN, the AR informs the CH about the new MN by sending a *Proxy Binding Update* to the CH and wait for a *Proxy Binding Acknowledgement* to add the new MN identifier in its cache. Here, MNs are expected to maintain their IPv6 addresses from their home network and allocated local addresses while moving under the mesh network coverage.

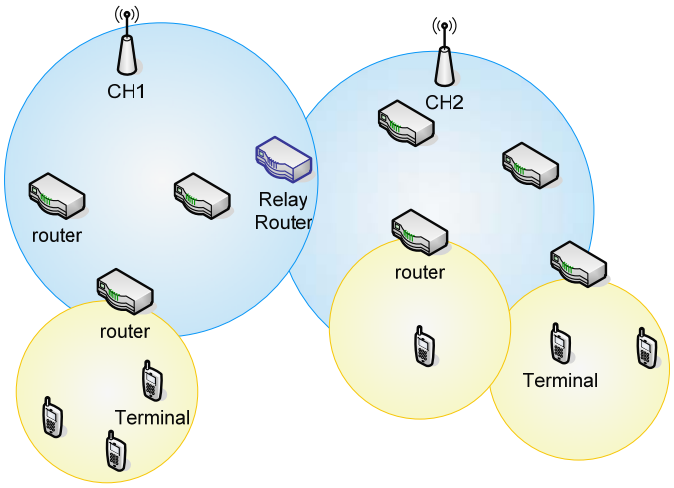

Figure 1. Cluster Based WMN Architecture

The paper is organized as follows: Section II provides related work including PMIPv6 protocol and existing movement detection mechanisms. Section III provides the guidelines and the design of our framework. Section IV introduce briefly on the virtual IPv6 wireless testbed using User-mode Linux and Ns-2 Emulation and some qualitative results. Section V concludes the paper.

II. RELATED WORK

A. *Proxy Mobile IPv6 (PMIPv6)*

PMIPv6 is designed to provide Network-based Mobility Management (NetLMM) to MNs having standard IPv6 stack [2][3][4]. It is assumed to support "unmodified" IPv6 MNs in the sense that no modification is required to the IP stack of MNs. Once an MN enters its PMIPv6 domain and attaches to an AR, the serving network can detect the attachment and detachment of the MN and emulate the home link on its new link.

That is, the serving network assigns a unique home network prefix to each MN, and conceptually this prefix always follows the MN wherever it moves within a PMIPv6 domain. From the perspective of the MN, the entire PMIPv6 domain appears as its home network.

The new principal functional entities of PMIPv6 are the Mobile Access Gateway (MAG) and Local Mobility Anchor (LMA). The MAG typically runs on the AR. The main role of the MAG is to detect the MN's movements and initiate mobility-related signaling with the MN's LMA on behalf of the MN. In addition, the MAG establishes a tunnel with the LMA for enabling the MN to use an address from its home network prefix and emulates the MN's home network on the access network for each MN. On the other hand, the LMA is similar to the HA in MIPv6. However, it has additional capabilities required to support PMIPv6. The main role of the LMA is to maintain reachability to the MN's address while it moves around within a PMIPv6 domain, and the LMA includes a binding cache entry for each currently registered MN. The binding cache entry maintained at the LMA is more extended than that of the HA in MIPv6 [5] with some additional fields such as the MN-Identifier, the MN's home network prefix, a flag indicating a proxy registration, and the interface identifier of the bidirectional tunnel between the LMA and MAG, etc. Such information associates the MN with its serving MAG, and enables the relationship between the MAG and the LMA to be maintained.

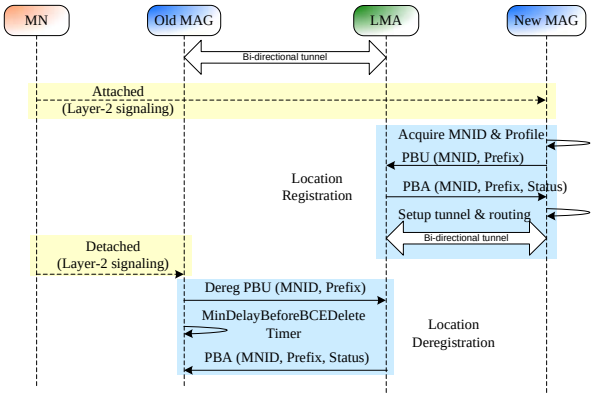

Figure 2. PMIPv6 Sequence Diagram

At any point, the MAG detects that the MN has moved away from its access link, or if it decides to terminate the MN's mobility session, it should start the Location Deregistration procedure by sending a *Proxy Binding Update* message to the LMA with the lifetime value set to zero.

Different approaches on the route optimization has been proposed, however no details on how to maintain the old session are provided

B. *Mobile Node Movement Detection*

An important aspect of any mobility protocol is the movement detection. Different movement detection mechanisms have been proposed for Mobile IP. However these are host-based and require special supports from the MN. For PMIPv6, the MAG must be responsible for the movement detection; this requires a network-based movement detection mechanism. The hints for movement detection can be the Link-Layer Event Notifications, Traffic Monitoring Events or DNAv6 [6]. Table 1 compares advantages and the drawbacks of different approaches:

Table 1. Comparison of Movement Detection Approaches

Hints	Advantages	Drawbacks
Traffic Monitoring Events	Independent from access technologies.	Processing overhead at MAGs.
Link-Layer Events	Accurate and Rapid.	Dependent on access technologies.
DNAv6	Independent from access technologies.	Dependent on how MN detect the attachment

A traffic monitoring based mechanism only works fine when there is uplink traffic from the MN to the network. The mechanism can be independent from the access technology but causes processing overhead at MAGs because MAGs must inspect every packet on the link. A link-layer event notification mechanism can be accurate and rapid. However in a heterogeneous environment, it depends on particular access technologies, requires a lot of modifications either on the network side or on the terminal side and therefore the deployment becomes difficult. DNAv6 also provides an IP-layer movement detection independent from access technology. DNAV6 uses the fact that the MN will send ICMPv6 message, e.g. Neighbor Solicitation (NS), and/or Router Solicitation (RS), when it move to a new link, which depends on how the MN detect the attachment and detachment.

An enhanced network-based IP-layer movement detection is a must to complement existing mechanisms for a short term evolution.

III. GUIDELINES AND DESIGN

A. *Basic Guidelines and Motivation*

We extend PMIPv6 to provide mobility and scalability in WMNs in a cluster based manner. In our architecture, the MAG typically runs on the AR and the LMA runs on the CH. Therefore AR and CH can be interpreted as MAG and LMA and vice versa dependently on the context.

B. *Cluster-based Architecture*

The cluster-based architecture consists of clusters (see Figure 3). Each cluster should have one and only one Cluster Head (CH) which has the LMA functionality and complete knowledge about group membership and link state information in the cluster. A relay router connects two adjacent clusters. Access Routers (ARs), control heterogeneous radio access technologies and provide access to MNs. The backhaul between the CH and the ARs in the infrastructure can be wired or wireless. The MN, which attaches to the AR, can be connected through the backbone to all other ARs. The MN therefore can communicate with other mobile Correspondent Nodes (CNs) through ARs as well as with CNs on the Internet through CHs.

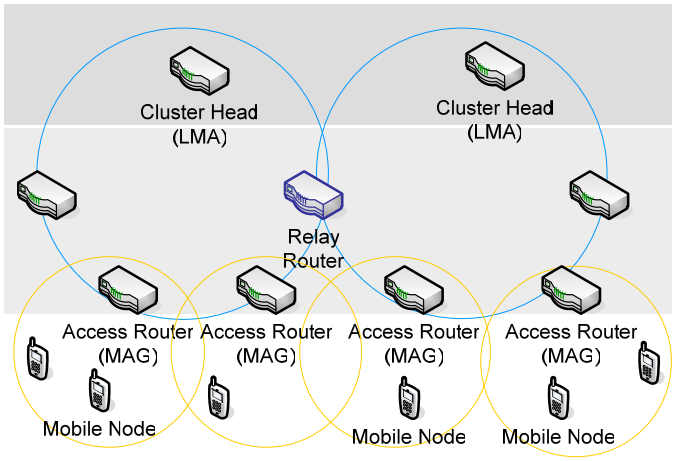

Figure 3. Scalability with Cluster-based Architecture

This type of architecture is also applied in Wireless Mesh Networks. In the case of wireless backhaul, we have a Cluster Based WMN which can minimize the updating overhead during topology change due to mobility of mesh nodes. If route optimization is considered, the traffic from one source MN to another destination MN should be able to pass through the relay router without passing through CHs. Details on route optimization are out of scope of this paper.

C. *Extended Proxy Mobile IPv6*

The standard Proxy Mobile IPv6 provides a natural solution for communication between the MN and the CN outside the PMIPv6 domain. It also works fine for intra-cluster communication between two MNs in the same cluster and intra-mobility. However for inter-cluster communication, when the MN and the CN belong to different clusters in the same PMIPv6 domain, one fundamental issue is that of locating the serving MAG or the serving LMA of the CN. As for inter-cluster mobility, when the MN moves from one cluster to a new cluster, it is necessary to activate the Location Deregistration procedure in the old cluster to maintain up-to-date routing information.

When establishing the communication between an MN and a CN belonging to different clusters, the serving MAG of the MN needs to know the serving MAG or the serving LMA of the CN. This issue is expressed as the problem of mapping a CN address into its serving MAG address or serving LMA address. This issue also arises in the case of route optimization in which the traffic could be forwarded directly from a source MAG to a destination MAG without passing through LMAs.

We propose a new couple of messages: *Proxy Binding Request* (PBReq) and *Proxy Binding Response* (PBRes) and a new mobility header option, named Serving MAG Address option (see Figure 4).

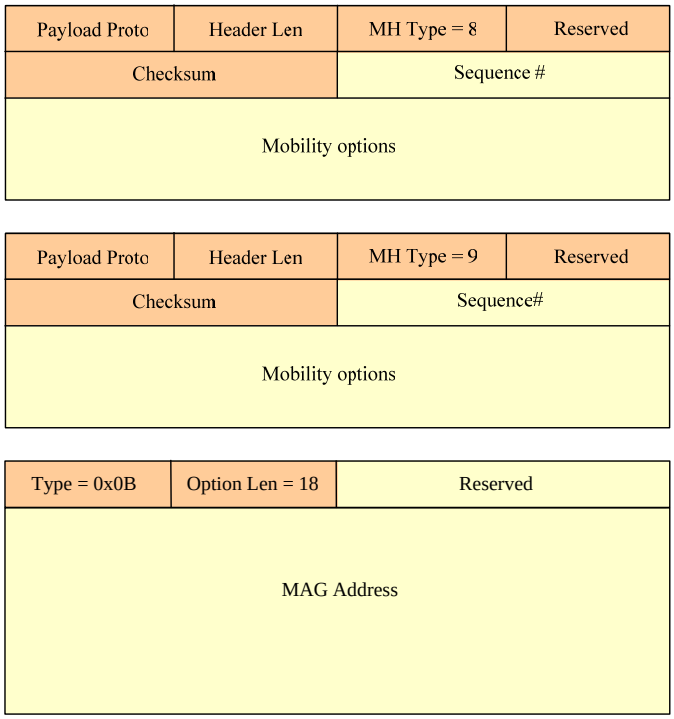

Figure 4. New messages and options for PMIPv6

The *Proxy Binding Request* message structure is similar to that of Binding Refresh Request of Mobile IPv6 except that the MH Type takes a value of 8 instead of 0. The value should be registered at IANA. This message is sent by the LMA to an All-LMA multicast group, an All-MAG multicast group, or to a centralized LMA to find which MAG is serving a mobile CN. The *Proxy Binding Response* message has similar structure as that of Proxy Binding Update except that the MH Type takes a value of 9. It responses to a PBReq and contains Serving MAG Address option which is a mandatory.

D. *Mobile Node Attachment*

Once an MN enters a cluster and attaches to an access link, the AR on that access link, after identifying the MN and acquiring its identity, will determine if the MN is authorized for the network-based mobility management service. If yes, the AR start the Location Registration procedure to update the CH about the current location of the MN.

Figure 5 shows a normal Location Registration process which is triggered by an MN Attachment event. The AR sends PBU to the CH and wait for the PBA, which include the Home Network Prefix of the MN, from the CH. The MN later can configure an address using any address configuration mechanism that is allowed in the network. Here we assume a Stateless Address Configuration [7]. Once the MN is attached to the cluster, it can reach all other attached MNs as in F or H sections.

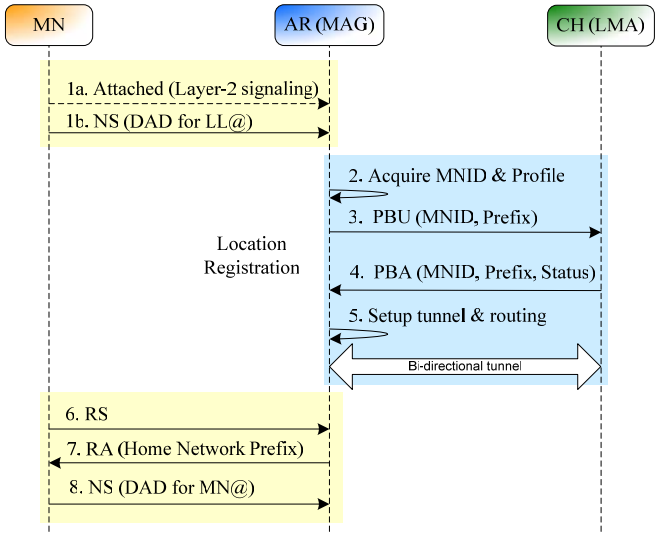

Figure 5. MN Attachment

E. Enhanced Network-based IP-layer Movement Detection

We propose here an algorithm for network-based IP-layer movement detection in heterogeneous wireless environment.

Precondition. In standard PMIPv6, the MN maintains an IP address that is unchanged within the PMIPv6 domain and is used for communications. This address is a global routable IP address and is referred in this paper as PMIPv6 address.

In our proposal, each AR broadcast Router Advertisements (RAs) containing two prefixes: (i) a global prefix P which is assigned to each MN (per-MN prefix) or is shared by all MNs (multi-link subnet with shared prefix) and (ii) a site-scope prefix P*. The global PMIPv6 address is configured from the global prefix P while the temporary site-scope IP address is configured from the site-scope prefix P*.

Whenever the MN moves to a new link, it configures a new temporary address and deletes the previous temporary address when its preferred lifetime is expired. The NS message in Duplicate Address Detection (DAD) process for this new temporary address is used as a trigger for the network attachment detection. Also note that the MAG does not need to wait for the completion of this DAD process. The following assumptions are taken into account.

Assumption 1: the MAG could extract the MNID, e.g. the MAC address or public key, from any ICMPv6 messages sent by the MN, e.g. Neighbor Solicitation (NS), Router Solicitation (RS), and Neighbor Advertisement (NA). Besides, there exists a bidirectional conversion between the MNID and the PMIPv6 address. Given a PMIPv6 address, we can infer the MNID and vice versa.

Assumption 2: If multiple addresses are active for the same interface, depending on the destination address, the source address of the communication is selected according to the Source Address Selection algorithm in RFC 3484 [8].

The first assumption allows the MAGs to detect the hints for network attachment of the MN when the MAG receives an ICMPv6 message. The second assumption ensures that the MN always prefer the PMIPv6 address for communications even when multiple addresses co-exist and therefore global prefix P and temporary site-scope prefix P* could be broadcasted by the AR on the same link.

Algorithm description. With the above precondition, each MN will have two IPv6 addresses: one is PMIPv6 address, which is a global IPv6 address and is unchanged within the PMIPv6 domain; another is the temporary address, which is a site-scope IPv6 address and is reconfigured whenever the MN moves from the old AR to a new AR. Here is the event-driven pseudo code:

```
on receiving a NS(target) for DAD
begin
  Extract target
  Compute MNID = get_MNID(NS)
  Compute PMIPv6 address = get_Address(MNID)
    if there is no PMIP binding entry for the MNID
    begin
      if get_Prefix(target) = P*
      begin
        Send NS (with target= PMIPv6 address) for ARP
        Create a "temporary" PMIP binding entry with a lifetime T*
      end
      else if get_Prefix(target) = P
        output Attachment Event (MNID)
    end
end
on receiving a NA(target) which replies the NS for ARP
begin
  Extract target
  Compute MNID=get_MNID(NA)
  if there exists a "temporary" PMIP binding entry for the MNID
    if get_Address(MNID) = target
      output Attachment Event (MNID)
end
on Attachment Event (MNID)
begin
  Start Location Registration Procedure (MNID)
  if there exists a "temporary" PMIP binding entry for the MNID
    Set the PMIP binding entry to "permanent"
  else if there is no PMIP binding entry for the MNID
    Create a "permanent" PMIP binding entry
end
on T* expired
begin
```

Delete the associated "temporary" PMIP binding entry

end

Thanks to the temporary site-scope prefix P* in Router Advertisement messages, sent periodically by the AR, the MN configures temporary site-scope address and activate DAD procedure by sending an NS message. This message will be used as a hint for the new AR to verify if the MN is really attached to it. The new AR activates the Neighbor Unreachability Detection (NUD) procedure by sending NS for address resolution with the target set to PMIPv6 Address. It also creates a temporary binding cache entry for the MN with a short life time and waits for the NA. If the MN has really moved inside the coverage of the new AR and associate with the new AR at the link layer, it must be able to answer this NS with an NA as a default behavior of Neighbor Discovery for IP Version 6 (NDPv6) [9]. The NA message, with the PMIPv6 address as the target, confirms the attachment of the MN and activates the Location Registration procedure.

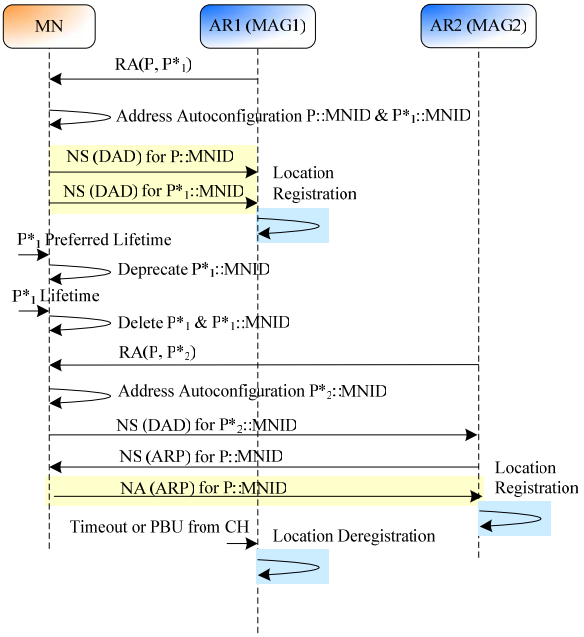

Figure 6. Example of Enhanced Network-based IP-Layer Movement Detection

Figure 6 shows a sequence diagram of a typical handover scenario, with enhanced network-based IP-layer movement detection, in which the MN first comes to the PMIPv6 domain (using a shared prefix) and attaches to the AR1. Later, the MN moves away from AR1 and attaches to the AR2.

F. Intra-cluster Communication Establishment

An MN can communicate with a Correspondent Node (CN) in the same cluster, i.e. intra-cluster communication, in an optimal way. The fundamental issue is that of locating the serving AR of one CN. This issue is expressed as the problem of mapping a CN Address into its Serving Access Router Address.

Both Nodes use the same network prefix. The MN sends an NS (Neighbor Solicitation) message to get the IP address of the CN. The MN's associated Access Router checks via its clusterhead the AR of attachment of the CN: *Proxy Binding Request* and *Proxy Binding Response* message exchange. The route is then established between the two access routers under the responsibility of the CH. The MN's AR acts then as a proxy for the IP packets transmission. Actual routing in the Cluster is done via establishment of MPLS tunnels. The description of this mechanism is out of scope of this paper.

G. Intra-cluster Mobility

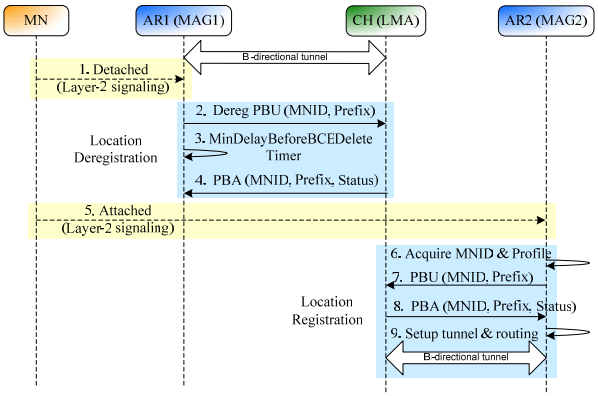

Figure 7. Intra-cluster Mobility

At any point, the AR detects that the MN has moved away from its access link, or if it decides to terminate the MN's mobility session, it start the Location Deregistration procedure by sending a *Proxy Binding Update* message to the CH with the lifetime value set to zero. After detecting a new MN on its access link, the AR must identify the MN and acquire the MN Identifier. If it determines that the network-based mobility management service needs to be offered to the MN, it must send a *Proxy Binding Update* message to the CH to start the Location Registration procedure.

Upon accepting this *Proxy Binding Update* message, the CH sends a *Proxy Binding Acknowledgement* message including the MN's home network prefix. It also creates the Binding Cache entry and sets up its endpoint of the bi-directional tunnel to the CH mobile access gateway. The AR, on receiving the *Proxy Binding Acknowledgement* message, sets up its endpoint of the bi-directional tunnel to the CH and also sets up the data path for the MN's traffic. At this point the AR will have all the required information for emulating the MN's home link. It sends *Router Advertisement* messages to the MN on the access link advertising the MN's home network prefix as the hosted on-link-prefix. For route optimization with MPLS tunnels, the CH also need to update existing MPLS tunnels for optimized on-going session of the MN.

H. Inter-cluster Communication Establishment

The communication path between an MN and a CN belonging to two separate clusters follows the same philosophy as the Intra-Cluster communication establishment.

When establishing the MPLS path between an MN and a CN belonging to different clusters, the AR serving the MN

needs to know the serving AR of the CN, and therefore triggers a chain of *Proxy Binding Request* and *Proxy Binding Response* messages. It relies on the fact that CH nodes are linked through relay nodes. *Proxy Binding Request* and *Proxy Binding Response* message exchanges are propagated through the chain of CH Nodes. This results in a route connecting the MN's AR and the CN's AR via MPLS tunnels traversing one or several relay nodes in the network.

This can be done with one centralized Home Agent (HA) with a traditional Client/Server architecture, in which the CHs play the role of the client and the HA plays the role of the server which provides the Serving Access Router Address Lookup service to all CHs. Another approach is to use broadcast/multicast between CHs to find out the Serving Access Router Address. When the network scale is very large, it could consume time and network resources to find out the Serving Access Router Address. A complement schema would be using peer-to-peer based approach in which all CHs form a peer-to-peer overlay network and provide the Serving Access Router Address Lookup service to other CHs. Here we consider the approach of using broadcast/multicast for a good trade-off between complexity and performance.

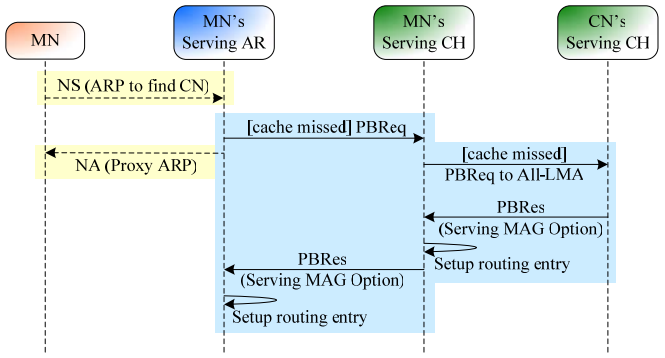

Figure 8. Inter-cluster communication establishment

The establishment for inter-cluster communication is described as in Figure 8. Any NS message for Address Resolution (ARP) will be inspected by the edge entities which are ARs. As the CN address is stored in the target field, these entities can look up the target in its binding cache to check if it is the serving entity of the CN. If the serving AR of the MN doesn't have any information about the target which belongs to the same PMIPv6 domain, i.e. cache missed, the AR assumes that the CN is away from its link and will send a PBReq message to the serving CH of the MN. The serving AR of the MN will also perform Proxy ARP for the CN. If the serving CH of the MN doesn't have any information about the target, it must send a PBReq to All-LMA multicast address. The serving CH of the CN will be able to answer with a PBRes carrying a Serving MAG Address Option.

The route is then established, under the responsibility of the CHs, for connecting the MN's serving AR and the CN's serving AR via MPLS tunnels traversing one or several relay nodes in the network. Once the path is set up, the traffic between the MN and the CN can be delivered.

I. Inter-cluster Mobility

When the MN moves between two ARs belonging to two different clusters, the inter-cluster mobility happens. As the old CH may not be aware about the changes, the new CH can send a PBRes message to All-LMA multicast address. This message helps the old CH to activate the Location Deregistration procedure if necessary, and helps other CHs to maintain up-to-date routing information, especially MPLS paths in case of route optimization, to keep on-going session.

IV. EXPERIMENTS AND RESULTS

A. Virtualization with UML and Ns-2 Emulation

In order to keep the results closest to the real experiment, we used a virtualization based testbed, using a combination of User-mode Linux (UML) [10][11] and Ns-2 Emulation [12], which would allow migrating to the real testbed with just insignificant efforts.

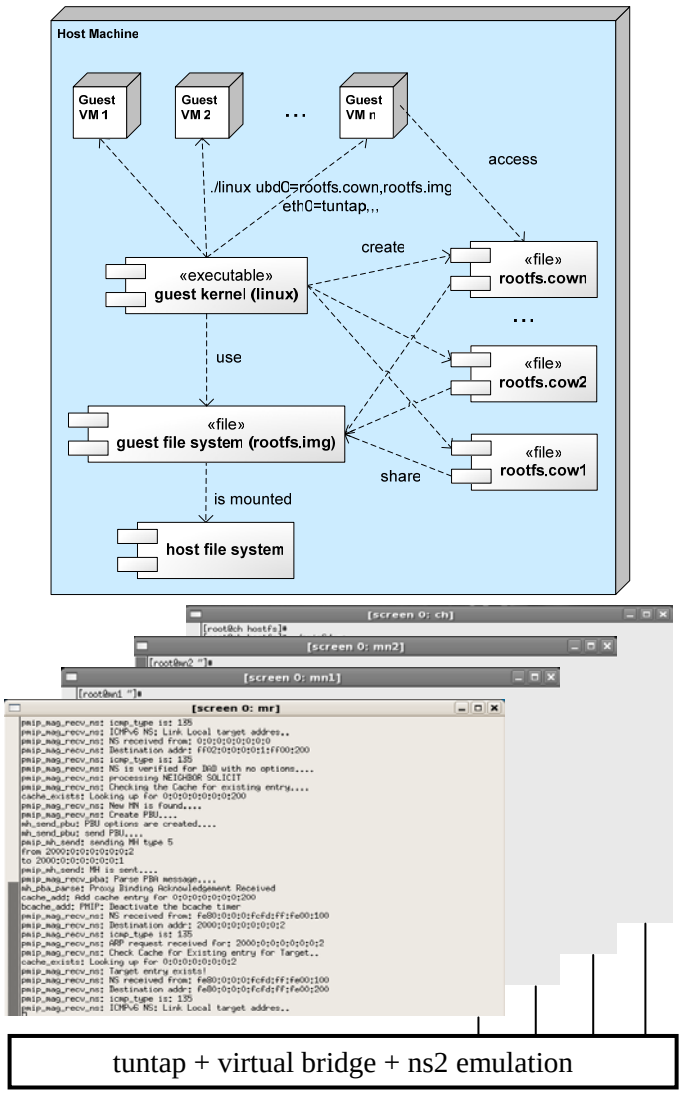

Figure 9. User-mode Linux and Ns-2 Emulation

UML is a Linux kernel which is compiled to run as a virtual machine on a Linux host. The virtual machine, called the guest to distinguish with the real host machine, can be assigned a guest root file system and other virtual physical resources different from the host machine. A UML virtual machine requires a guest kernel and a guest root file system. The guest root file system of an UML is stored in a file on the real host machine.

The Ns-2 Emulation feature is used to emulate the wireless environment. It can grab packets from source virtual machine (real IPv6 stack), pass them through a simulated wireless network, and then inject them back into the destination virtual machine. Each Ns-2 node in the Ns-2 simulated network represents a virtual Ethernet interface (TAP device) in the network.

B. PMIPv6 Implementation

We implemented PMIPv6 on top of Mobile IPv6 for Linux (MIPL) v2.0 [13]. All the basic bricks of MIPL are reused in an efficient way as shown in Figure 10. In MIPL v2.0, Mobile IPv6 is implemented using multi threads: One thread for handling the ICMPv6 messages, one thread for handling Mobility Header messages, one thread for handling tasks and time events, etc.

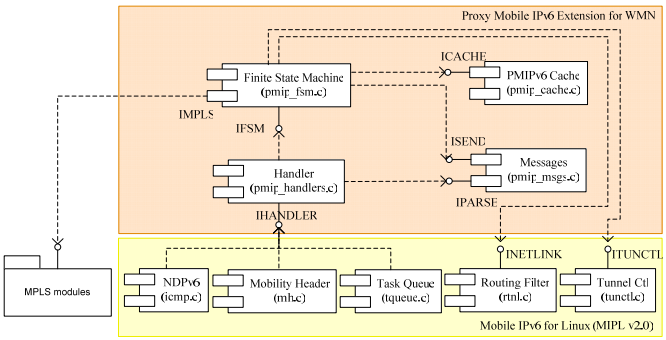

Figure 10. PMIPv6 Software Architecture

To support PMIPv6, we extend these elements and implement handlers for all necessary messages and events. All ICMPv6 messages or Mobility Header messages are parsed as the input to the finite state machine, which is the heart of the system. This finite state machine makes appropriate decisions and controls all other elements to provide a correct predefined protocol behavior. As PMIPv6 implementation is built on top of MIPL version 2, it could be later integrated in MIPL easily and grows in line with the standards as well as MIPL source code.

C. Virtual IPv6 WMN testbed

The virtual testbed in this early phase is composed of one cluster with one CH, two routers AR1 and AR2. A CN, positioned in the Internet, is connected directly with the CH. There are two MNs which don't have any specific software to support the mobility. Initially, MN1 is attached to AR1 and MN2 is attached to AR2. IEEE 802.11 is used for the virtual wireless link.

Figure 11 shows the virtual Wireless Mesh testbed. The topology is defined and generated using Virtual Network User-Mode Linux (VNUML)[14]. Scenarios are defined and automated with Tcl language which is a part of Ns-2 Emulation.

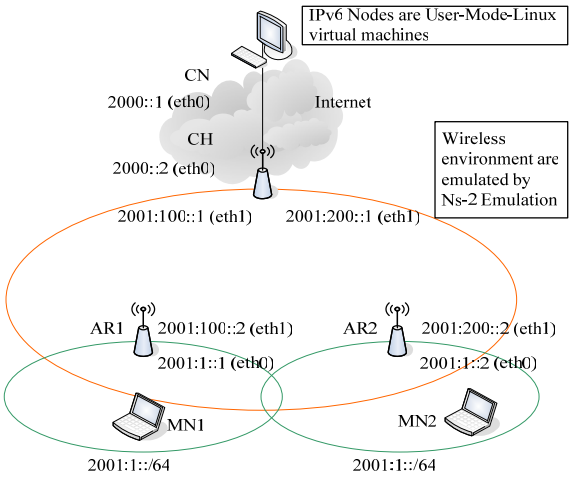

Figure11. Virtual Wireless Mesh Testbed

D. Qualitative Results

Different test scenarios are defined and carried out to verify the correctness of the framework. Table 2 shows the main scenarios that have been tested.

Table 2. Test Scenarios

Scenarios	Descriptions	Results
Attachment Detection	MN1 and MN2 come inside AR1 coverage	Successful registration of MN1/MN2 in both AR1& CH
Detachment Detection	MN1 or MN2 turns down the interface (or moves away from AR1).	The cache entry is deleted in both AR1 and CH.
Intra-link Com-munication	MN1, MN2 are attached to AR2. Traffic between MN1 and MN2	MN1 can communicate with MN2
Intra-cluster Com-munication	MN1 is attached to AR1. MN2 is attached to AR2. Traffic between MN1 and MN2	The traffic is encapsulated through AR1-CH and AR2-CH tunnels.
Mobility and Movement Detection	MN1 moves from AR1 to AR2. The PMIPv6 address of MN1, which is configured with the PMIPv6 prefix, is kept unchanged. MN1 configures new	AR2 detects the attachment and starts the registration procedure. AR1 detects the detachment and starts the

	temporary address, and deletes the old temporary address.	deregistration procedure. Session continuity is assured. On-going sessions can continue
Inter-cluster Com-munication	A test bed of 7 nodes with 2 clusters. AR1 is under control of CH1, AR2 is under control of CH2. 2 clusters are connected through a Relay. MN1 is attached to AR1. MN2 is attached to AR2. Traffic between MN1 and MN2 is created.	MN1 can communicate with MN2

V. CONCLUSIONS

We extended PMIPv6 for Cluster Based Heterogeneous WMNs. The framework can support network-based mobility to MNs having standard IPv6 stack. A new enhanced network-based IP-layer mechanism was proposed. This movement detection mechanism allows detecting the attachment and the movement of each MN independently from the access technologies and requires no special support from the MN. We implemented and deployed the framework in a virtual IPv6 wireless mesh testbed and provide some qualitative results to prove the correctness and the advantages of the framework.

The proposed framework is suitable for different kinds of applications. One of current applications is to deploy rapidly a mobile and wireless communication environment in Integrating Communications for enhanced environmental risk management and citizen's safety (FP7 CHORIST) [15] European safety and communications between rescue actors. The framework combines different hot trends in mobile networking to form a realistic and practical platform for future advanced mobile networking researches. Another application is to spontaneously structure the communication backbone of community based networks (French AIRNET project of the ANR – Agence Nationale pour la Recherche) [16].

Our future work will concentrate on inter-cluster communication and inter-cluster mobility, on route optimization as well as on QoS support. Performance evaluation with quantitative results will also be realized.

The developments are integrated in the framework of the EURECOM's Open Source Platform "OpenAirInterface"[17].

VI. ACKNOWLEDGEMENTS

Eurecom Institute's research is partially supported by its industrial members: BMW, Cisco Systems, France Télécom, Hitachi Europe, SFR, SHARP, STMicroelectronics, Swisscom, Thales. Authors are also thankful to Hussain Ahmed, Paul Marie Joseph Venmani Daniel Philip, Lamia Romdhani (EURECOM) and Hirokazu Naoe (SHARP) for help and valuable advices.

VII. REFERENCES

[1] M. Portmann and A. A. Pirzada, "Wireless Mesh Networks for Public Safety and Crisis Management Applications," *IEEE Internet Computing*, vol. 12, no. 1, pp.18 25, January/February, 2008.
[2] J. Kempf, "Goals for network-based localized mobility management (netlmm)," RFC 4831, April 2007.
[3] J. Kempf, "Problem statement for network-based localized mobility management," RFC 4830, April 2007.
[4] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, "Proxy Mobile IPv6," RFC 5213, August 2008.
[5] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6," RFC 3775, Jun 2004.
[6] J. Kempf, S. Narayanan,E. Nordmark, B. Pentland and JH. Choi, "Detecting Network Attachment in IPv6 Networks (DNAv6)," Internet draft (work in progress), February 2008.
[7] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration," RFC2462, December 1998.
[8] R. Draves, "Default Address Selection for Internet Protocol version 6 (IPv6)," RFC 3484, February 2003.
[9] T. Norten, E. Nordmark and W. Simpson, "Neighbor Discovery for IP Version 6," RFC2461, December 1998.
[10] User Mode Linux Home Page, http://user-mode-linux.sourceforge.net
[11] Nguyen, Huu Nghia; Bonnet, Christian, "Practical and unified process for developing the future Mobile Internet with Simultaneous Access (MISA)," Research Report RR-08-211, February 2008.
[12] Daniel Mahrenholz and Svilen Ivanov, "Real-Time Network Emulation with ns-2," *Proceedings of The 8-th IEEE International Symposium on Distributed Simulation and Real Time Applications, Budapest Hungary*, October 21-23, 2004.
[13] Mobile IPv6 for Linux, http://www.mobile-ipv6.org
[14] Virtual Network User Mode Linux home page http://www.dit.upm.es/vnumlwiki/index.php/Main_Page.
[15] CHORIST Project Home Page, http://www.chorist.eu.
[16] AIRNET Project Home Page, http://www.rnrt-airnet.org/
[17] OpenAirInterface Home Page, http://www.openairinterface.org